AMENDMENTS TO THE CLAIMS

The listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims

1. (Currently Amended) An encryption apparatus for a common-key cipher, comprising:

a unit for generating a plurality of plaintext blocks P_i $(1 \leq i \leq N)$ resulting from separating a plaintext P on a specific-length basis, the plaintext including ~~redundant data and~~ a message M;

an encryption operation unit for generating [[a]] random-number blocks R_i $(1 \leq i \leq N+1)$ ~~string R~~ from a secret key, wherein the number of the random-number blocks R_i is greater than that of the plaintext blocks P_i, ~~generating random-number blocks R_i $(1 \leq i \leq N+1)$ from the random-number string R,~~ and performing an encryption operation for ciphertext blocks C_i $(1 \leq i \leq N)$ ~~$(1 \leq i \leq N+2)$~~ by using the plaintext blocks P_i $(1 \leq i \leq N)$ and the random-number blocks R_i $(1 \leq i \leq N)$ ~~$(1 \leq i \leq N+1)$~~, wherein the number N of the random number blocks is the same as that of the ciphertext blocks; ~~the random-number string R being is longer than the plaintext, and wherein the random-number blocks R_i $(1 \leq i \leq N+1)$ being used for the encryption correspond corresponding to the plaintext blocks P_i $(1 \leq i \leq N)$; and~~

a unit for generating a message-authentication-code of the ciphertext blocks C_i $(1 \leq i \leq N)$ by using the ciphertext blocks C_i $(1 \leq i \leq N)$ and the random-number blocks R_i (where $2 \leq i \leq N+1$) among the generated random-number blocks Ri, wherein the number N of the random-number blocks is the same as that of the ciphertext blocks; and

an output unit for generating and outputting a ciphertext C comprising the ciphertext blocks and the message-authentication-code.

~~an authentication operation unit for~~

~~generating random-number blocks R_i $(2\leq i\leq N+1)$ from the random-number string R, and~~

~~performing an authentication operation for message-authentication-code blocks by using the ciphertext blocks C_i $(1\leq i\leq N+2)$ and the random-number blocks R_i $(2\leq i\leq N+1)$, the random-number blocks R_i $(2\leq i\leq N+1)$ being used for the authentication corresponding to the ciphertext blocks C_i $(1\leq i\leq N+2)$.~~

2. (Cancelled)

3. (Cancelled)

4. (Currently Amended) The encryption apparatus for a common-key cipher according to Claim 1, [[2,]] wherein:

the encryption operation unit is configured to perform ~~performs~~ the encryption operation by using an exclusive-OR logical sum, and to output the ciphertext blocks having a length the same as that of the plaintext blocks; and

the message-authentication-code generation unit ~~authentication operation unit~~ is configured to perform ~~performing~~ the authentication operation by using an arithmetic multiplication and an arithmetic addition, and to output the message-authentication-code comprising message-authentication-code blocks C_{N+1} and C_{N+2} having a length two times longer than that of the ciphertext blocks.

5. (Currently Amended) The encryption apparatus for a common-key cipher according to Claim 1, [[2,]] wherein:

the encryption operation unit is configured to perform ~~performs~~ the encryption operation by using an exclusive-OR logical sum, and to output the ciphertext blocks having a length the same as that of the plaintext blocks; and

the message-authentication-code generation unit ~~authentication operation unit~~ is configured to perform an ~~performing the~~ authentication operation by a multiplication on a finite field, and to output message-authentication-code comprising message-authentication-code blocks C_{N+1} and C_{N+2} having a length two times longer than that of the ciphertext blocks.

~~and an arithmetic addition.~~

Claims 6-9. (Cancelled)

10. (Currently Amended) A decryption apparatus for a common-key cipher, comprising:

a unit for generating a plurality of ciphertext blocks C_i $(1 \le i \le N)$ and a message authentication-code by ~~C'_i $(1 \le i \le N+2)$ resulting from~~ separating a ciphertext C on a specific-length basis;

an authentication operation unit configured for:

(a) generating [[a]] random-number string R from a secret key, wherein the number of the random-number blocks R_i is greater than that of the ciphertext blocks, ~~generating random-number blocks R_i $(1 \le i \le N+1)$ from the random-number string R, and~~

(b) generating ~~performing an authentication operation for~~ message-authentication-code blocks of ciphertext blocks C_i $(1 \le i \le N)$ by using the ciphertext blocks C_i $(1 \le i \le N)$ ~~C'_i $(1 \le i \le N+2)$~~ and the random-number blocks R_i (where $2 \le i \le N+1$), ~~$(1 \le i \le N+1)$,~~ wherein the number N of the random-number blocks is the same as that of the ciphertext blocks, and

~~the random-number string R being longer than the ciphertext, the random-number blocks R_i $(1 \leq i \leq N+1)$ being used for the authentication corresponding to the ciphertext blocks C'_i $(1 \leq i \leq N+2)$; and~~

(c) comparing the message-authentication-code blocks generated from the ciphertext blocks with the message-authentication code blocks included in the ciphertext blocks;

a decryption operation unit for, if the authentication operation has succeeded, ~~generating random-number blocks R_i $(1 \leq i \leq N)$ from the random-number string R, and~~ performing a decryption operation ~~for~~ to obtain plaintext blocks P_i [[P'_i]] $(1 \leq i \leq N)$ by using the ciphertext blocks C_i $(1 \leq i \leq N)$ ~~C'_i $(1 \leq i \leq N+2)$~~ and the random-number blocks R_i $(1 \leq i \leq N)$ among the random-number blocks Ri, wherein the number N of the random-number blocks is the same as that of the ciphertext blocks; and

an output unit for outputting a plaintext P comprising the plaintext blocks P_i $(1 \leq i \leq N)$.

~~, the random-number blocks R_i $(1 \leq i \leq N)$ being used for the decryption corresponding to the ciphertext blocks C'_i $(1 \leq i \leq N+2)$.~~

11. (Cancelled)

12. (Currently Amended) The decryption apparatus for a common-key cipher according to Claim 10, [[11,]] wherein the decryption operation unit does not perform the decryption operation, if the authentication operation has failed.

Claims 13-23. (Cancelled)

24. (New) The decryption apparatus for a common-key cipher according to claim 12, wherein:

the message-authentication included in the ciphertext has a length two times longer than the ciphertext blocks;

the authentication operation unit is configured to perform the authentication operation by using an arithmetic multiplication, and outputs the message-authentication-code comprising message-authentication-code blocks C_{n+1} and C_{n+2}, wherein the message-authentication-code has a length two times longer than that of the ciphertext blocks; and

the decryption operation unit is configured to perform the decryption operation by using an exclusive-OR logical sum, and to output the plaintext blocks having a length the same as that of the ciphertext blocks.

25. (New) A computer-readable medium having stored thereon instructions which, when executed by a processor, cause the processor to perform the steps of:

generating a plurality of plaintext blocks P_i ($1 \leq i \leq N$) resulting from separating a plaintext P on a specific-length basis, the plaintext including a message M;

generating random-number blocks R_i ($1 \leq i \leq N+1$) from a secret key, wherein the number of the random-number blocks R_i is greater than that of the plaintext blocks P_i;

performing an encryption operation for ciphertext blocks C_i ($1 \leq i \leq N$) by using the plaintext blocks P_i ($1 \leq i \leq N$) and the random-number blocks R_i ($1 \leq i \leq N$) wherein the number N of the random number blocks is the same as that of the ciphertext blocks;

generating a message-authentication-code of the ciphertext blocks C_i ($1 \leq i \leq N$) by using the ciphertext blocks C_i ($1 \leq i \leq N$) and the random-number blocks R_i (where $2 \leq i \leq N+1$) among the generated random-number blocks Ri, wherein the number N of the random-number blocks is the same as that of the ciphertext blocks; and

generating and outputting a ciphertext C comprising the ciphertext blocks and the message-authentication-code.

26. (New) The computer-readable medium according to Claim 25, further comprising the steps of:

performing the encryption operation by using an exclusive-OR logical sum;

outputting the ciphertext blocks having a length the same as that of the plaintext blocks;

performing the authentication operation by using an arithmetic multiplication and an arithmetic addition; and

outputting the message-authentication-code comprising message-authentication-code blocks C_{N+1} and C_{N+2} having a length two times longer than that of the ciphertext blocks.

27. (New) The computer-readable medium according to Claim 25, further comprising the steps of:

performing the encryption operation by using an exclusive-OR logical sum;

outputting the ciphertext blocks having a length the same as that of the plaintext blocks;

performing an authentication operation by a multiplication on a finite field; and

outputting the message-authentication-code comprising message-authentication-code blocks C_{N+1} and C_{N+2} having a length two times longer than that of the ciphertext blocks.

28. (Currently Amended) A computer-readable medium having stored thereon instructions which, when executed by a processor, cause the processor to perform the steps of:

generating a plurality of ciphertext blocks C_i ($1 \leq i \leq N$) and a message authentication-code by separating a ciphertext C on a specific-length basis;

generating random-number string R from a secret key, wherein the number of the random-number blocks R_i is greater than that of the ciphertext blocks;

generating message-authentication-code blocks of ciphertext blocks C_i ($1 \leq i \leq N$) by using the ciphertext blocks C_i ($1 \leq i \leq N$) and the random-number blocks R_i (where $2 \leq i \leq N+1$), wherein the number N of the random-number blocks is the same as that of the ciphertext blocks;

comparing the message-authentication-code blocks generated from the ciphertext blocks with the message-authentication code blocks included in the ciphertext blocks;

performing, if the authentication operation has succeeded, a decryption operation ~~for~~ to obtain plaintext blocks P_i ($1 \leq i \leq N$) by using the ciphertext blocks C_i ($1 \leq i \leq N$) and the random-number blocks R_i (where $1 \leq i \leq N$) among the random-number blocks Ri, wherein the number N of the random-number blocks is the same as that of the ciphertext blocks; and

outputting a plaintext P comprising the plaintext blocks P_i ($1 \leq i \leq N$).

29. (Currently Amended) The computer-readable medium according to Claim 28, wherein the decryption operation unit does not perform the decryption operation, if the authentication operation has failed.